

# C1000-197 Online Tests & New C1000-197 Study Materials

Pass IBM C1000-197 Exam | Latest C1000-197 Dumps & Practice Exams - Cert007

1. Where should administrators first look when Guardium anomaly detection is not producing expected results?

- A. Baseline configuration settings on collectors
- B. Appliance firmware version history
- C. Report builder custom templates
- D. LDAP server connection logs

**Answer: A**

2. What two tasks should administrators schedule to maintain long-term appliance performance? (Choose two)

- A. Periodic log rotation and cleanup
- B. Manual shutdowns after each policy update
- C. Continuous disabling of anomaly detection
- D. Regular firmware and patch updates

**Answer: AD**

3. Which two steps must be taken to configure Guardium groups effectively for access and policy management? (Choose two)

- A. Assign members based on database roles or departments
- B. Create groups only on aggregators for scalability
- C. Define group-specific permissions and roles
- D. Restrict groups to a single appliance only

**Answer: AC**

4. Which two elements must be configured when defining a Guardium policy for monitoring sensitive queries? (Choose two)

- A. Policy rules with specific conditions
- B. Enforcement actions such as alert or block
- C. Appliance firmware upgrade schedules
- D. Database license type allocation

**Answer: AB**

5. Which factor is critical when planning integrations between Guardium and ticketing systems like ServiceNow?

- A. Ensuring that Guardium supports SNMP traps
- B. Confirming API compatibility for automated incident creation
- C. Assigning the ticketing system as a collector appliance
- D. Using Guardium's central manager to run ServiceNow scripts

**Answer: B**

6. What is the purpose of Guardium Installation Manager (GIM)?

- A. Facilitating installation, updating and configuration of agents.
- B. Capturing change audit information of configuration files and more on the database server.
- C. Specifying the database platform and the instances that the S-TAP monitors on the S-TAP host.

2 / 4

If you purchasing our C1000-197 simulating questions, you will get a comfortable package services afforded by our considerate after-sales services. We respect your needs toward the useful C1000-197 practice materials by recommending our C1000-197 Guide preparations for you. Only in a few minutes, your ordered C1000-197 exam questions are sent to you, and whenever you have any question on the C1000-197 practice guide, you can contact with our service at 24/7.

Considering all customers' sincere requirements, C1000-197 test question promise to our candidates with plenty of high-quality products, considerate after-sale services. Numerous advantages of C1000-197 training materials are well-recognized, such as 99% pass rate in the exam, free trial before purchasing, secure privacy protection and so forth. From the customers' perspective, We treasure every customer's reliance and feedback to the optimal C1000-197 Practice Test and be the best choice.

>> C1000-197 Online Tests <<

## 100% Pass Quiz 2026 IBM C1000-197 Realistic Online Tests

Our C1000-197 test guide is test-oriented, which makes the preparation become highly efficient. Once you purchase our C1000-197 exam material, your time and energy will reach a maximum utilization. Thus at that time, you would not need to be afraid of the society and peer pressure with C1000-197 Certification. In conclusion, a career enables you to live a fuller and safer life. So if you want to take an upper hand and get a well-pleasing career our C1000-197 learning question would be your best friend.

## IBM Guardium Data Protection v12.x Administrator - Professional Sample Questions (Q53-Q58):

### NEW QUESTION # 53

What two steps should administrators take when maintaining Guardium policies to adapt to changing threats? (Choose two)

- A. Review policy violation trends regularly
- B. Require firmware reinstallation each time
- C. Adjust policy rules based on new database risks
- D. Disable all existing policies before updates

Answer: A,C

### NEW QUESTION # 54

Which two Guardium components are essential when planning for centralized management and policy distribution in a large enterprise? (Choose two)

- A. Collector appliance
- B. Central manager appliance
- C. Aggregator appliance
- D. Standalone S-TAP agent

Answer: A,D

### NEW QUESTION # 55

When should administrators configure Guardium to forward alerts to a SIEM instead of relying solely on internal dashboards?

- A. When anomaly detection is disabled
- B. When only one database is monitored in the environment
- C. When enterprise-wide incident correlation and monitoring are required
- D. When S-TAP agents are offline

Answer: C

### NEW QUESTION # 56

Why is it important to synchronize Guardium appliances with an NTP server?

- A. To control CPU frequency for performance optimization
- B. To automatically reset appliance passwords on schedule
- C. To trigger database discovery scans at fixed intervals
- D. To ensure logs and reports have consistent timestamps across appliances

Answer: D

### NEW QUESTION # 57

How can administrators confirm that Guardium S-TAP agents remain compatible with updated database versions during maintenance?

- A. Allow S-TAPs to self-update without verification
- B. Disable S-TAPs whenever databases are patched
- C. Test S-TAP connectivity using aggregator appliances
- D. Check IBM Guardium compatibility matrices before upgrades

Answer: D

